

Bugku writeup

原创

老青蛙38324 于 2019-03-03 15:30:48 发布 190 收藏

文章标签: [Bugku writeup](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/weixin_44119209/article/details/88088674

版权

Bugku题目 writeup (一)

一些小的体会

在做 **ctf** 题目时要选择合适的浏览器, 火狐或者是谷歌, 一些常用插件搞清楚, 前期做题靠工具, 后期做题靠实力, 注意自身知识的积累与总结

一.杂项

1.签到题

关注得到 **flag**

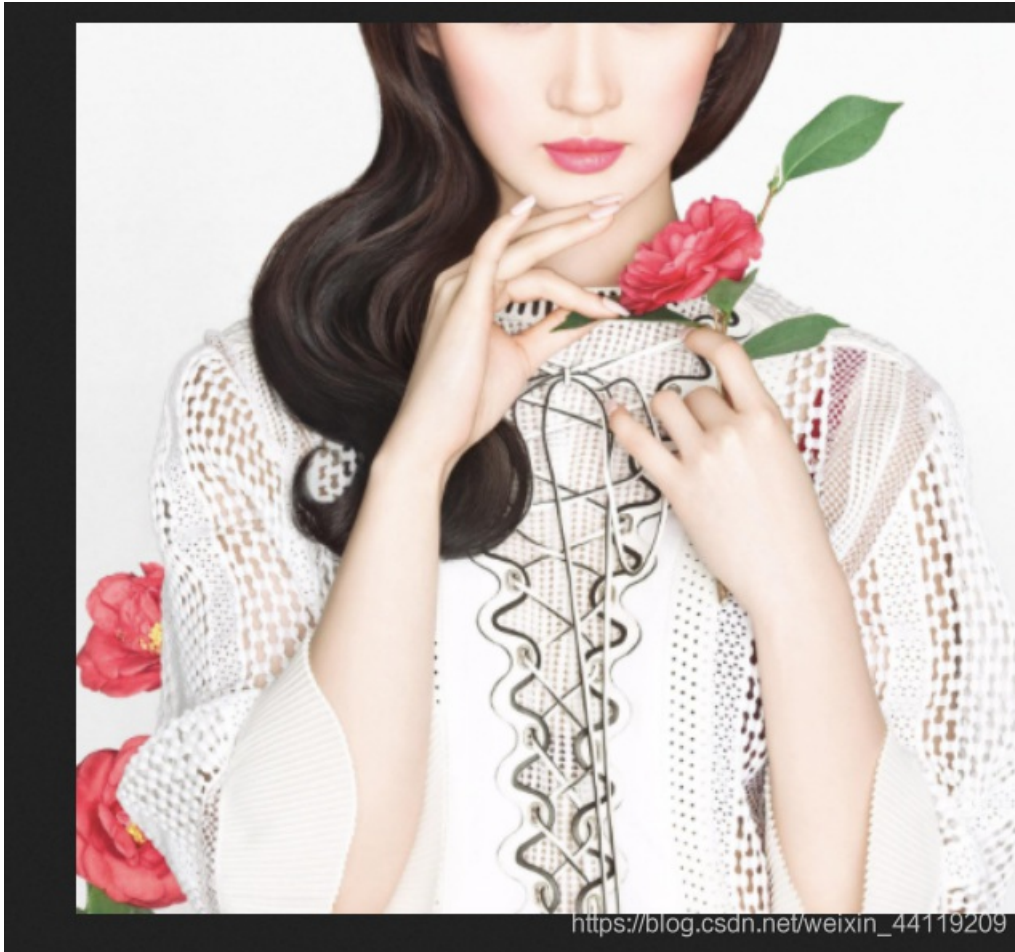
2.这是一张单纯的图片

用 **winhex** 打开图片, 发现一串数字, **ascii** 码转码, 得到 **flag**

```
Š ŷ&#107;&#101;  
&#121;&#123;&#12  
1;&#111;&#117;&#  
32;&#97;&#114;&#  
101;&#32;&#114;&  
#105;&#102;&#104
```

3.猜

百度有一个智能识图功能, 识别一下, 刘亦菲的大名就出来了



二.WEB

1.web2

打开网站一堆滑稽，**F12**，得到**flag**。

```
<body id="body" onload="init()">  
  <!--flag KEY{Web-2-bugKssNNikls9100}-->  
  <script type="text/javascript" src="js/ThreeCanvas.js"></script>  
  <script type="text/javascript" src="js/Snow.js"></script>  
  <script type="text/javascript">...</script>
```

![在这里插入图片描述](https://img-blog.csdnimg.cn/20190303152156568.png?x-oss-process=image/watermark,type_ZmFuZ3poZW5naGVpdGk,shadow_10,text_aHR0cHM6Ly9ibG9nLmNzZG4ubmV0L3dlaXhpbl80NDExOTlwOQ==,size_16,color_FFFFFFFF,t_70)

2.计算器

发现框内只能输入一位数字，**F12**打开开发者工具，修改网页**html**，改成相应的位数，输入答案，得到**flag**。

43+61=?

验证

```
查看器 控制台 调试器 {} 样式编辑器 性能 内存 网络 存储
DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/
border:1px solid #e2b4a2;
background: #e2b4a2;
}
.input {
width: 100px;
}
</style>
</head>
<body>
<span id="code" class="code" style="background: rgb(254, 137, 236) none repeat scroll 0% 0%;
141);">43+61=?</span> <input type="text" class="input" maxlength="3">
<button id="check">验证</button>
```



3.web基础get

读懂代码，还是要好好学习语言，构造？ **what=flag**得到**flag**

```
← → ↻ 🏠 123.206.87.240:8002/get/?what=flag  
$what=$_GET['what'];  
echo $what;  
if($what=='flag')  
echo 'flag{****}';  
flagflag{bugku_get_su8kej2en}
```

https://blog.csdn.net/weixin_44119209

4.矛盾

从php代码中可读出矛盾，php判断字符串以1开头即可判断等值，构造**num=1**，**zl**表示字符串连接即可

```
← → ↻ 🏠 123.206.87.240:8002/get/index1.php?num=1zl  
$num=$_GET['num'];  
if(!is_numeric($num))  
{  
echo $num;  
if($num==1)  
echo 'flag{*****}';  
}  
1zlflag{bugku-789-ps-ssdf}
```

https://blog.csdn.net/weixin_44119209

5.web3

打开网页对话框一只弹出，阻止，查看一下页面源代码，在最后发现一串编码，解码得到**flag**

```
130 alert("来找我吧");  
131 alert("flag就在这里");  
132 alert("来找我吧");  
133 <!--&#75;&#69;&#89;&#123;&#74;&#50;&#115;&#97;&#52;&#50;&#97;&#104;&#74;&#75;&#45;&#72;&#83;&#49;&#49;&#73;&#73;&#73;&#125;-->  
134 </script>  
135 </head>  
136 /<!--&#75;&#69;&#89;&#123;&#74;&#50;&#115;&#97;&#52;&#50;&#97;&#104;&#74;&#75;&#45;&#72;&#83;&#49;&#49;&#73;&#73;&#73;&#125;-->
```

6.web5

提交随便一个密码，出现再好好看看，burpsuite直接抓包，出现一些字符，百度后发现有jother编码，谷歌console回车得到**flag**

server: nginx
date: Sun, 03 Mar 2019 07:13:33 GMT
content-type: text/html
connection: close
content-length: 12539

<html>

<body>

<div

style="display:none;">$1+2+3+\dots+n = \frac{n(n+1)}{2}$</div></body></html>